**Name - Gaurang A Raorane Roll No - 49**

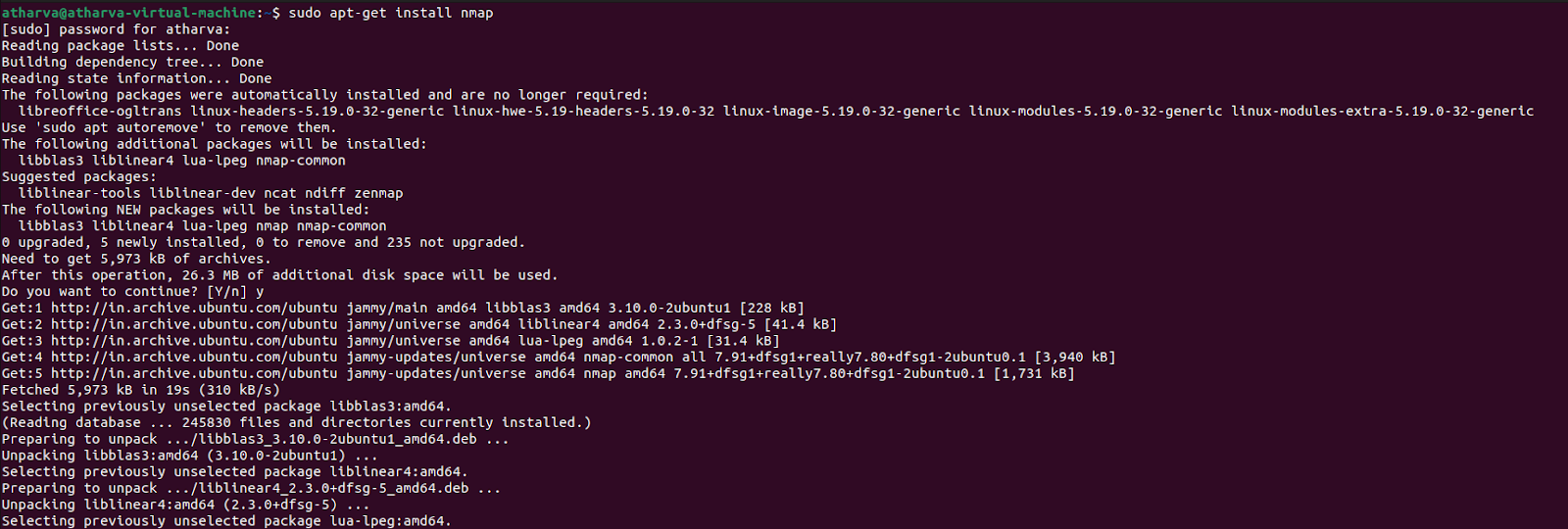
**Class - D15A Batch - C**

**CA EXPERIMENT 1**

**Aim:** Download, install nmap and use it with different options to scan open ports, perform OS fingerprinting, ping scan, tcp port scan,udp port scan, etc.

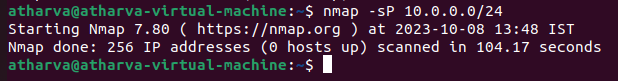
**1)** Installation of nmap:

$sudo apt-get install nmap



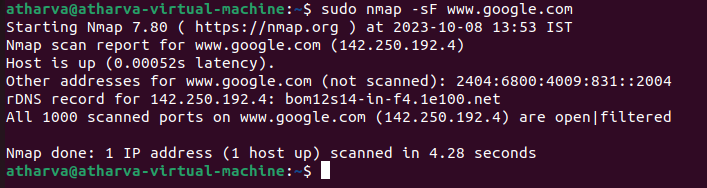
**2)** $nmap -sP 10.0.0.0/24

Ping scans the network, listing machines that respond to ping.



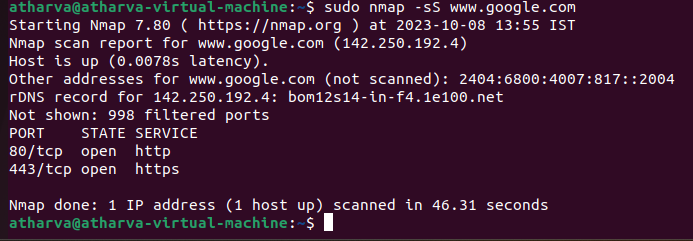
**3)** FIN scan (-sF). Sets just the TCP FIN bit.

$sudo nmap -sF [www.google.com](http://www.google.com)



**4)** Scan IP addresses and ports of a website or server

$sudo nmap -sS [www.google.com](http://www.google.com)

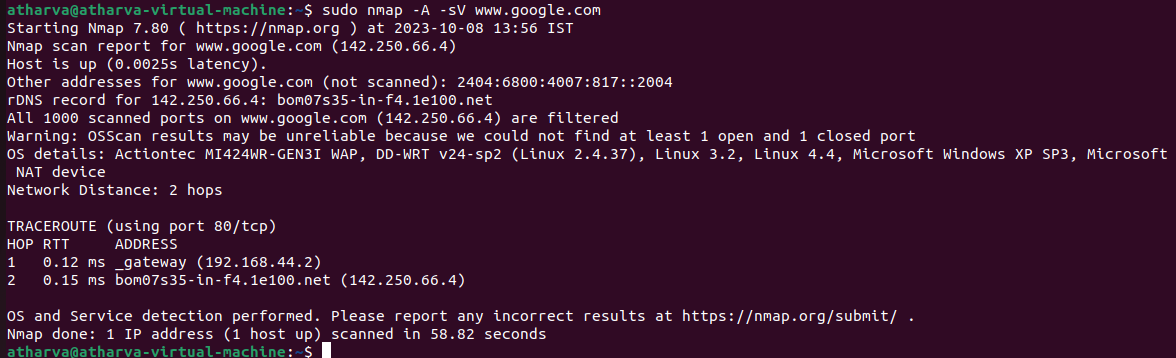
****

**5)** -sV (Version detection):

Enables version detection, as discussed above. Alternatively, can use -A, which enables

version detection among other things.

$sudo nmap -A -sV [www.google.com](http://www.google.com)



**6)** -sO (IP protocol scan) .

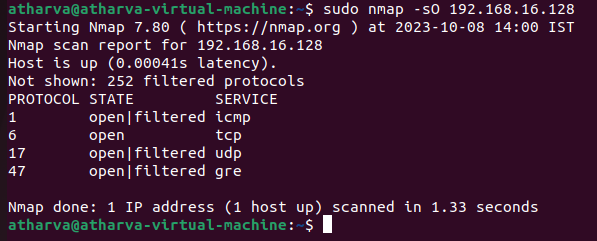
IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.)

are supported by target machines. This isn't ́t technically a port scan, since it cycles

through

IP protocol numbers rather than TCP or UDP port numbers.

$sudo nmap -sO 192.168.16.128

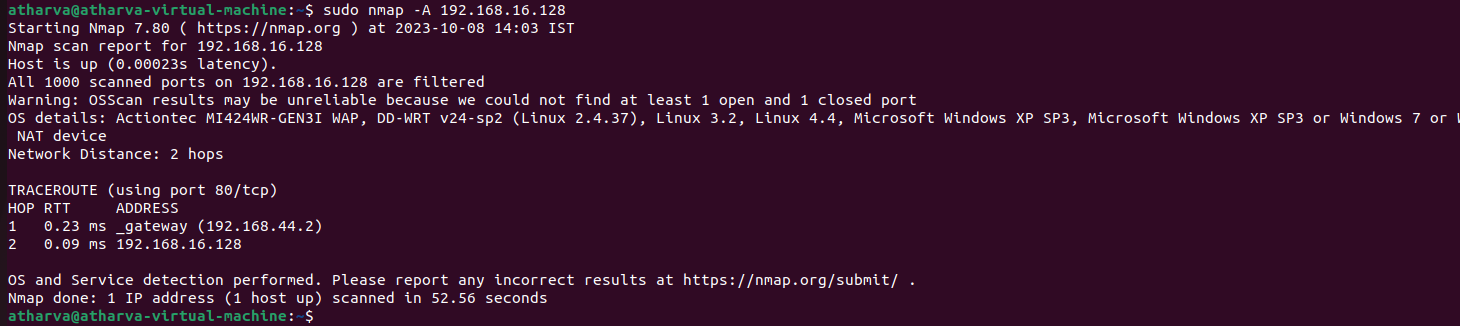


**7)** -O (Enable OS detection) .

Enables OS detection, as discussed above. Alternatively, you can use -A to enable

OS detection along with other things.

$sudo nmap -A 192.168.16.128



**8)** -p port ranges (Only scan specific ports) .

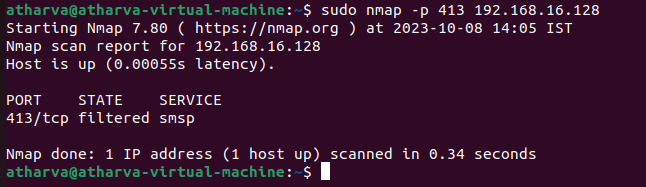
This option specifies which ports you want to scan and overrides the default. Individual

Port numbers are OK, as are ranges separated by a hyphen (e.g. 1-1023). The beginning

and/or end values of a range may be omitted, causing Nmap to use 1 and 65535,

respectively.

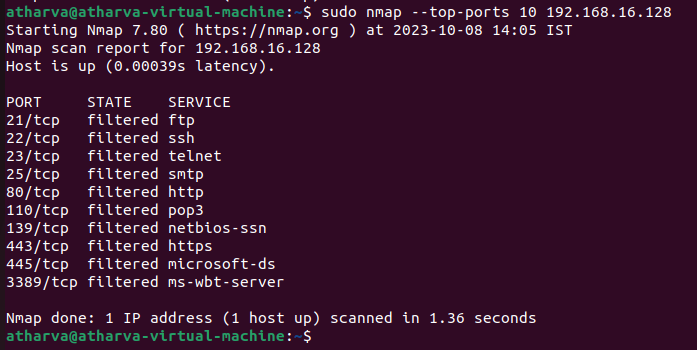
$sudo nmap -p 413 192.168.16.128



**9)** --top-ports <integer of 1 or greater>

Scans the N highest-ratio ports found in nmap-services file.

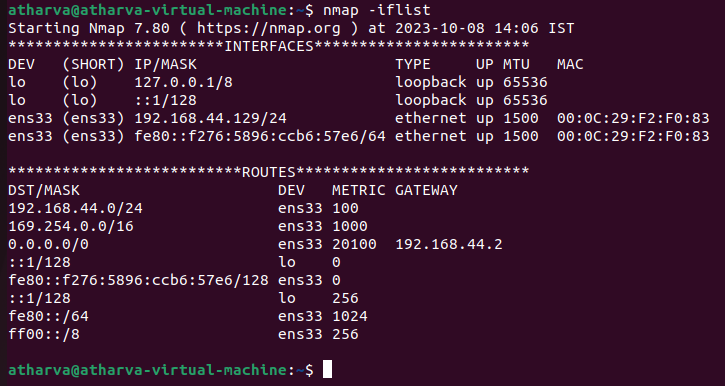
$sudo nmap --top-ports 10 192.168.16.128



**10)** nmap –iflist

Host interface and route information with nmap by using –iflist option.

$nmap -iflist



Conclusion :- Successfully installed nmap and performed various commands to scan open ports and also perform OS fingerprinting.